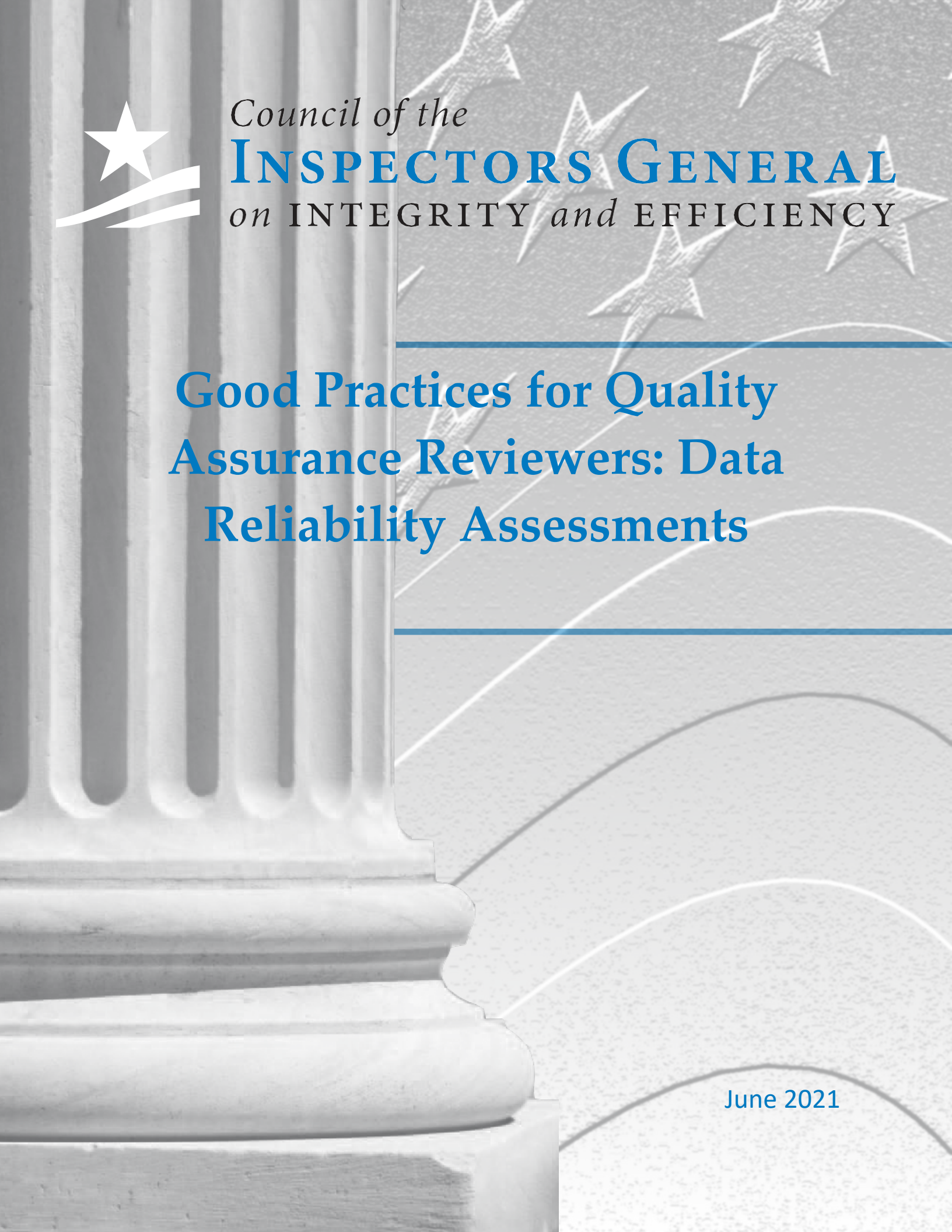


Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Good Practices for Quality Assurance Reviewers: Data Reliability Assessments

June 2021

EXECUTIVE SUMMARY

Objective

The purpose of this white paper is to share good practices related to reviewing a team's data reliability assessment.

Approach

One of QAWG's goals is to identify and document good practices to help the OIG community improve QA functions. To implement this goal, QAWG, through FAEC, sent a survey in July 2019 to senior OIG audit leadership and managers to identify key areas of concern about the application or interpretation of performance audit standards. Data reliability was identified as an area of concern. The QAWG formed a task team to identify and summarize good practices for reviewing data reliability assessments for performance audits.

This white paper provides an overview of data reliability assessment (DRA) based on guidance from the U.S. Government Accountability Office's (GAO) Assessing Data Reliability, GAO-20-283G (GAO's Guidance), as well as the experience of multiple OIG and audit professionals. The purpose is to share good practices quality assurance (QA) reviewers can use to assess a performance audit team's DRA. Specifically, this guidance includes information on what documentation a QA reviewer can expect to see as part of the audit team's data reliability testing and reporting requirements. The guidance also includes examples and clarification of terms and expectations.

The Government Auditing Standards (GAS) 2018 Revision (Yellow Book), requires auditors to assess the completeness and accuracy of data significant to the audit objectives. The audit file should demonstrate the audit team reviewed the evidence objectively and independently and considered it in context to determine when the threshold of sufficiency and appropriateness was met. As the volume and technical nature of evidence increases, it can be difficult to determine what is required for DRA or how to review the DRA. The key to DRA is to determine if the data can be used as intended. The process and types of evidence a QA reviewer can expect to see in a DRA include gathering source information, system documentation, conducting interviews, testing electronic records, and corroboration. Not all are needed every time. This is a matter best decided by the audit team using their professional judgment.

The guidance in this white paper is not prescriptive; each QA reviewer should consider the agency's unique policies and procedures and use professional judgment in assessing the agency's implementation and compliance with professional standards. In addition, this white paper should not be considered a replacement or supplement to generally accepted government auditing standards, and it should not be considered as a basis for an external peer review result.

INTRODUCTION

In October 2016, representatives from various Federal Offices of Inspector General (OIG) formed the Quality Assurance Working Group (QAWG) to enhance and improve the quality assurance (QA) review processes used by the Federal OIG community. In January 2019, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) formally recognized QAWG as part of the Federal Audit Executive Council (FAEC).[1] One of QAWG's goals is to identify and document good practices to help the OIG community improve their QA functions. To implement this goal, QAWG, through FAEC, sent a survey in July 2019 to senior OIG audit leadership and managers to identify key areas of concern about the application or interpretation of performance audit standards. QAWG formed task teams to develop separate white papers that address the top five identified areas of concern.[2, 3]

Purpose

This white paper presents good practices QA reviewers can use to assess a performance audit team's data reliability assessment. It includes information on what documentation a QA reviewer can expect to see as part of the audit team's data reliability testing and reporting requirements. The guidance also includes DRA examples and clarification on DRA-related terms.

The guidance in this white paper is not prescriptive; each QA reviewer should consider the agency's unique and procedures and use professional judgment in assessing the agency's implementation and compliance with professional standards. In addition, this white paper should not be considered a replacement or supplement to generally accepted government auditing standards, and it should not be considered as a basis for a peer review result.

Background

Audits often rely on data as evidence. This requires auditors to assess the reliability of the data they are using – i.e., its accuracy, completeness, and applicability for the purposes of the audit. The auditor's assessment should result in the team developing a good understanding of how the data is collected, the systems they are extracted from, and the relevant information systems controls for key data elements.[4] The primary focus of a data reliability assessment is to determine whether the data can be used for the audit's intended purposes – to determine the reliability of the specific data needed to support the findings, conclusions, and recommendations in the

[1] FAEC is a subgroup established by CIGIE to discuss and coordinate issues affecting the Federal audit community, with special emphasis on audit policy and operations of common interest to members.
[2] The survey results identified the top concerns of OIG senior leadership and management where professional standards were not being consistently interpreted: (1) audit risk, (2) data reliability, (3) sampling, (4) supervisory review, and (5) quality assurance. They also identified internal controls as a key concern, which is being addressed by CIGIE's internal controls working group.
[3] GAO, *Assessing Data Reliability* (GAO-20-283G) was issued in December 2019 and was therefore not available to the OIG community prior to the survey that queried OIGs on which topics could benefit OIGs by sharing good practices.
[4] GAO, *Assessing Data Reliability*.

context of the audit objectives.[5]

A DRA is different than an information systems audit, which is an audit of controls related to an information systems to determine the effectiveness of those controls in safeguarding corporate assets, maintaining the integrity of stored and communicated data, supporting corporate objectives effectively, and operating efficiently. A review of information systems internal controls may be needed when significant to the audit objectives, as shown in Appendix A, Example 2. In this case, auditors should follow the guidance provided in the Yellow Book (GAS 8.59-8.62).

Criteria

The Yellow Book requires audit teams assess the sufficiency and appropriateness of computer processed information, regardless of whether this information is provided to auditors or they extract it independently.[6] Attributing the data to its source does not alleviate the need for auditors to assess the reliability of the data. GAO published a guide, *Assessing Data Reliability* (GAO-20-283G), to assist auditors in assessing the reliability of data. It provides a risk-based framework for data reliability assessments that can be geared to the specific circumstances of each engagement. Each audit organization's policies and procedures should provide additional guidance on how audit teams should document and assess the data.

GAO's Standards and Guidance

The term "data reliability" is mentioned only once in the Yellow Book, and it is in the context of information systems and the reliability of computer-generated information. GAS 8.67 states that auditors may decide to evaluate the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. Specifically, GAS 8.67c states that the relationship of information systems controls to data reliability may factor into auditors' assessments of whether these controls are significant to the audit.[7] GAS 8.67c further states:

> *To obtain evidence about the reliability of computer-generated information, auditors may decide to evaluate the effectiveness of information systems controls as part of obtaining evidence about the reliability of the data. If the auditors conclude that information systems controls are effective, they may reduce the direct testing of data.*

However, GAS 8.98 establishes the importance of the DRA by stating that the sufficiency and

[5] GAO-20-283G, p. 2.
[6] GAS 8.90-8.96.
[7] Information systems controls include general controls, application controls, and user controls. Auditors can assess the potential significance of information systems controls in conjunction with internal controls or separately, depending on the audit's objectives (GAS 8.61-8.67). The assessment includes the design, implementation, and operating effectiveness of these controls. When information systems controls are deemed significant, auditors need to design "steps to obtain sufficient, appropriate evidence to support the audit findings and conclusions," and consider the extent to which they must test the effectiveness of the controls to answer the audit objective (GAS 8.60-8.62).

appropriateness of data from external sources should be reviewed regardless of how it was obtained. The assessment includes reviewing the completeness and accuracy of the data based on its planned use.

Another significant section, GAS 9.17, is related to data but not specifically to data reliability. GAS 9.17 addresses the report quality elements of accuracy and completeness:

- **Accuracy.** An accurate report is supported by sufficient, appropriate evidence with key facts, figures, and findings that are traceable to the audit evidence. Disclosing data limitations and other disclosures contribute to producing more accurate audit reports.

- **Completeness.** Being complete means clearly stating what was and was not done, explicitly describing the data limitations and constraints imposed by restrictions on access to records.

GAO's Guidance is a comprehensive guide on how to conduct and document the DRA. A major tenet of the guidance is the essential role of professional judgment in each of the three stages of the DRA:

(1) deciding whether a DRA is necessary
(2) determining the extent of the DRA
(3) making the final determination of reliability

According to GAO's *Assessing Data Reliability*, the use of professional judgment is an essential element of determining data reliability. Auditors use this critical mindset to assess data that may initially seem appropriate. Exercising professional judgment to determine the sufficiency and appropriateness of evidence is integral to the engagement process.

Agency's Internal Policies and Procedures

The QA reviewer should evaluate the audit team's compliance with the audit organization's policies and procedures on assessing data reliability. However, this white paper does not prescribe how to analyze the organization's policies and procedures.

EVIDENCE OF DATA RELIABILITY DOCUMENTATION

The QA reviewer should be able to follow and understand the audit team's assessment and documentation of data reliability that are relevant to the audit objective, including understanding any analysis and work performed. The QA reviewer will review the documentation to determine whether auditors clearly documented the data reliability methodology and testing to understand the conclusions and results, as suggested in GAO's Guidance.

Documenting the Data Reliability Assessment

The audit team should complete the initial DRA as early as possible in an audit. Early examination of data reliability helps the team determine whether the data are appropriate for addressing the audit objectives.[8] The data reliability assessment includes a range of possible steps for collecting information about data. These steps to assess the data should support the audit team's decision to use the data as part of their fieldwork.[9] For an overview, see Appendix B: The Assessing Data Reliability for Performance Audits Flowchart. The audit team should exercise professional judgement when deciding which information collection steps to incorporate into an assessment based on the circumstances of their particular audit.

As part of the evidence, the QA reviewer may expect to see the following steps conducted by audit teams as part of the data reliability assessment**.**

1. **Interviews.** Audit teams can conduct interviews with knowledgeable officials as part of assessing the reliability of data—for example, agency program officials, data managers, technical specialists, and others outside the agency who are knowledgeable about the data—to assess whether the data are applicable for audit purposes. The interviews may occur via multiple methods, including in person, phone, email, or a collaboration tool. The QA reviewer should look for documentation of the interviews which may include officials' statements about the following:

    - the population and time period of interest
    - variables related to the audit objectives
    - potential reliability issues with the data
    - the completeness and accuracy of the data
    - the systems controls surrounding the data or its system

2. **Review of data documentation**. Evidence of a data documentation review may include summaries and analysis of user manuals, data dictionaries, system documentation, table layouts, data entry and processing policies, data quality assurance program materials, and other relevant documentation. Auditors may also summarize evaluations of the data systems performed by others as a part of other projects, such as financial audit reports. The QA reviewer should look for conclusions the auditors make about the data from these documents, such as whether data entry controls seem sufficient to minimize errors or whether documented quality control steps, such as validation procedures, seem adequate given the type of data and how they will be used in the audit.

3. **Data testing**. As part of assessing the reliability of data, auditors may test data for accuracy and completeness. The QA reviewer should look for detailed explanations of the tests

[8] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 7: Additional Considerations, states "Early examination of data reliability helps the team determine whether the data are appropriate for addressing the audit objectives… To minimize last-minute challenges, auditors should address data reliability issues in the planning phase of engagements," p.34.
[9] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 4: Steps for Collecting Information When Assessing Data Reliability, p.17.

performed, including methodology and conclusions. The data tests conducted will vary for each assessment and can include the following:[10]

- evidence that the team determined the acceptable level of error and whether the accuracy of the data impacted the ability to answer the audit objective
- checking the total number of records provided against agency totals
- testing for missing data, either entire missing records or missing values in key data elements
- looking for duplicate records
- looking for invalid or duplicate identifiers
- testing for values outside a designated range
- looking for dates outside valid time periods or in an illogical progression
- looking for unexpected aspects of the data—for example, extremely high values associated with a certain geographic location
- testing relationships between data elements, such as whether data elements correctly follow a skip pattern from a questionnaire
- verifying that computer processing is accurate and complete, such as testing a formula used in generating specific data elements or testing to ensure that edit checks or validations are working correctly

4. **Tracing to source documents or other corroborating information.**[11] As part of the DRA, teams may Trace the data to source documents to compare data records and values to provide additional support for confirming the reliability of data, as well as identifying and quantifying the magnitude of any errors. Tracing can be performed by the audit team on entire record sets or a sample (random samples preferred).[12] The QA reviewer should look for clear descriptions of work performed along with supporting documentation.

5. **Conclusion.** Regardless of the form or content of the audit team's DRA, the QA reviewer should look for evidence of the audit team's conclusion about the reliability of the data and determination whether additional procedures or steps need to be added to the project as a

[10] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 4: Steps for Collecting Information When Assessing Data Reliability, p.21-22.
[11] Tracing is the process of ensuring that the numbers, formulas, and other data were accurate. Other OIGs refer to this as linking or cross-referencing.
[12] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 4: Steps for Collecting Information When Assessing Data Reliability, p.22.

result of the data determination. When applicable, the initial DRA should be updated to reflect any significant changes identified after completing the initial assessment.

- ***If the Data Are Reliable***

  If the data are considered reliable, the QA reviewer would expect to see the following:
  - the audit team's steps taken to complete the assessment, as stated above
  - compliance with the audit organization's documentation of the DRA
  - the data tested and the methodology used
  - a clear link from data reliability to the next steps to answer the audit objective(s), if applicable

- ***If the Data Are Not Reliable***

  If the data are not considered reliable, the QA reviewer would expect to see that evidence supports this conclusion and details any limitations included in the audit report, such as:
  - the documentation to support the analysis and steps taken to address the lack of reliable data to mitigate risk and ensure adequate controls
  - ways to mitigate risk, including expanding testing, changing the data source, conducting additional procedure steps, and changing the audit objectives
  - updating the DRA documentation with any conclusions reached

All work performed as part of a data reliability assessment should be documented by the audit team in a manner consistent with the audit organization's evidence standards. The documentation should be clear about what steps the audit team took and what conclusions they reached. Use of a standardized template for recording all documentation related to the data reliability assessment, while not required, can help improve consistency of assessments within the audit organization.[13]

Reporting on Data Reliability

If applicable, the QA reviewer should expect to see language in the audit report on the data reliability assessed and tested as part of the audit team's work and a determination whether the data were reliable or unreliable, or that the team could not determine reliability. When describing the methodology, audit teams should refer to the use and source of data; how data reliability was assessed; what was the determination of the assessment; and, if there were issues with the data, report those issues as needed to answer the audit objective(s). The documentation should support the scope and methodology and assessment made.[14] For examples of how the QA reviewer can evaluate the data reliability assessment, see Appendix A.

[13] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 7: Additional Considerations, p.34.
[14] GAS 8.93 and 8.94; GAO, *Assessing Data Reliability* (GAO-20-283G), Section 6: Including Appropriate Language in the Report, p.31.

Conclusion

Performance audits often require some degree of data reliability assessment. However, it is a matter of professional judgment to determine the specifics of each assessment, including whether a review of information systems internal controls is needed. Audit teams may have differing judgments on how to evaluate the available data based on the knowledge, skills, and expertise of all personnel involved in an engagement. It is a matter of the team's professional judgment to determine the extent of the review, what should be reviewed, and what is sufficient to complete the assessment. Documentation should be generated and maintained that demonstrates the DRA process and allows the QA reviewer to understand the decisions that led the audit team to its determination about data reliability.

APPENDIX A: EXAMPLES

The following are examples of data reliability assessments that the QA reviewer might expect to see. The actual documentation included in the project is a matter of professional judgment based on the audit objective. More or less documentation may be found in the projects based on the relevant circumstances of the project.

Example 1: Assess data for reliability to select the fieldwork sample

Audit Objective: Was a sample of government loans underwritten in compliance with rules and regulations?

Facts about the Audit

- The universe of loans resides on an agency server. The auditee selects a certain type of loan based on the audit team's parameters and downloads the data —1,000 loans. This file is provided by the agency to the audit team in Microsoft Excel.

- The audit team selects a sample of 30 loans from the file, based on relevant fields, to test data reliability.

- During the rest of the project (called "fieldwork" by some OIGs), the audit team reviews copies of the sampled loan files to address the objective.

- On review of the loan files, the team discovered that one loan was the wrong loan type and had to be removed from the sample.

Is a DRA required?

- Are the data expected to be significant to the findings? The sample was derived from a universe of loans and based on the accuracy of data in the fields. A DRA is required.

QA Reviewer Expectations for the DRA

- **Source Information.** Documentation identifies the information source (possibly system documentation), how the agency obtained assurance over the reliability of the data and confirmed that the information provided by the auditee matched the request (for example, does the loan type match the parameter the audit team requested).

- **Electronic Testing.** Evidence is clear that the team identified and tested relevant fields in the file for accuracy and completeness and provided a description of the tests conducted (search for duplicates, incorrect or error values, accurate date ranges, etc.).

- **Corroboration**. After the DRA was completed, the team reviewed actual loan files during the remainder of the project that corroborated the data reliability assessment.

However, one incorrect loan rendered the actual size of the loan universe unknown, which would prevent the team from projecting its findings without further reliability testing. The error pointed to a potential internal control weakness related to the accuracy of loan type, but that issue was beyond the scope of the audit. The QA reviewer could expect to see the DRA updated with the additional facts discovered in fieldwork.

- **Overall Assessment.** We determined that the data were reliable for audit purposes with the limitations described above, which are included in the audit report.

Example 2: When information systems controls are significant to the audit objectives

Audit Objective: Determine if the front-door screening process is effective

Facts about the Audit:

- Building entrants badge in through an electronic door. The scanner uses software to compare the employee's badge ID to the list of employees in Active Directory (AD) — a list of all workers who have an active email account in Outlook. The door opens for any worker with an account on the list.

- The Human Resources (HR) department, however, maintains the master list of all employees. The HR list is used to update the list of employees in AD.

Is a DRA required?

- Are the data expected to be significant to the findings? The AD list is used to determine who enters the building; therefore, confirmation of its accuracy is critical to understanding the effectiveness of the front door screening process. A DRA is required.

QA Reviewer Expectations for the DRA

- **Source Information.** Documentation identifying the system information source for the list of employees in the AD (system documentation if available), how the data was extracted, and confirmation that the number of records provided by HR matched the number in the AD.

- **Corroboration.** Evidence that the accuracy of the AD list was checked against its source—the list maintained by HR.

- **Information Systems Internal Controls.** Evidence that the audit team examined/tested internal controls designed to ensure the accuracy of the AD list. For example, determine if the related internal controls exist, and are they functioning properly? How is the AD list updated, manually or automatically? How often? How is it checked for accuracy?

- **Assessment.**[15] We determined that the data were reliable for audit purposes.

Example 3: When an audit report leverages information from a prior information systems controls assessment

Your OIG performed an in-depth assessment of the information systems controls of a contracting system and concluded that these controls were effective for the contracting system. As a result of the assessment, OIG can reduce the direct testing of data on the upcoming audits.

As the QA reviewer of the individual audits that leveraged the information systems controls assessment of the contracting system, you would expect to see:

- **the reference to** the prior information systems controls assessment of the contracting system

- **an explanation why** the earlier assessment of the contracting system is timely and relevant to the current audit, with due consideration of the following:

    - data fields, purposes, upgrades or changes to the system, and time periods that were assessed, as well as other issues that could affect previous assessment's relevance to the current engagement

    - if the scope of the data reviewed is not within the scope of the information systems controls assessment of the contracting system, the team will not be able to rely on the assessment to reduce testing.

- **an explanation how** data testing is limited or can be reduced by
    - the work that was done in the information systems controls assessment
    - the use of the data in the current audit
    - the risk associated with relying on the data

- **conclusions reached** on the use and applicability of the prior information systems controls assessment.

[15] When information systems internal controls are significant to the audit objectives, the Yellow Book requires auditors to evaluate the design, implementation, and effectiveness of the controls (GAS 8.60). In addition, "when internal control is significant in the context of the audit objectives, auditors should include the following in the audit report: (1) the scope of their work on internal control and (2) any deficiencies in internal control that are significant within the context of the audit objectives and based upon the audit work performed" (GAS 9.29).

Example 4: When data originated and were managed outside a U.S. government agency

Audit teams may come across data generated by a non–U.S. government agency[16] that resides outside their immediate geographical area (geographical limitations), making it challenging to conduct site visits. Gaining access to the data source can prove problematic in terms of its reliability, particularly if the audit team needs to depend on the data for reporting purposes. The audit team will still need to exercise due diligence to determine that the data are sufficiently reliable to move on to the next steps in their audit.

The QA reviewer should expect that the audit team documented the following:

- the steps taken by the audit team to test the data's reliability through interviews, review data documentation, evaluate the completeness of data, and verify the source
- additional steps taken to analyze data, including checking whether the source is reliable or cross-referencing data with the reporting of the U.S. government agency
- review of other controls built in to ensure that the data are reliable, such as evaluation of internal controls and overall risk analysis
- documentation of the audit team's approach consistent with the Yellow Book or other applicable standards and policies
- documentation of any management decision to limit testing
- how the data will be used in the audit
- the conclusion of the audit team on the reliability of the data and any limitations
- a detailed explanation of the steps taken by the audit team to satisfy fundamental data reliability issues and limitations to test the data further (scope and methodology)
- language in the report that aligns with the documentation that supports the analysis, conclusion, and limitations

Example 5: When data that supports the findings and conclusion lack source documents

As the QA reviewer, you are reviewing a project in which the audit team was unable to obtain the source documents that support the data the agency provided. In this case, the source documents were destroyed in a flood.

The QA reviewer can expect to see the following kinds of additional steps taken by the audit team to assess the reliability of the data:

[16] A non–U.S. government agency can be an international organization, a non-government organization, or a foreign entity conducting work on behalf of the U.S. government.

- Documentation of the reason why the source documents were not available, and whether that increased the internal control and audit risks, as well as any steps taken to address these areas:

    - exceptions should be noted, including information escalated to relevant officials about the lack of source documentation.

    - if audit risk is increased, the steps taken to reduce that risk to an acceptable level.

- Documentation supporting the team's conclusion on the reliability of the data, which could include the following:

    - information from knowledgeable officials

    - documentation about the system and processes—a more in-depth examination of internal controls

    - heavier reliance than usual on electronic data testing

    - the team's professional judgment as to the overall reliability and why it is or is not acceptable to rely on the data in the context of the audit's objective(s) and any expected findings and conclusions

Example 6: When a data reliability assessment is not needed

If the data are not material to support your findings, conclusions, and recommendations, the audit team does not need to assess data reliability.[17] This example is a compliance review for FY 2020 grants.

Audit Objective: Was the oversight of an FY 2020 grant in compliance with requirements?

Facts about the Audit:

- According to the data, the agency spends about $10 million annually on grants.
- The auditors identified potential issues with the administration of grants in another audit.

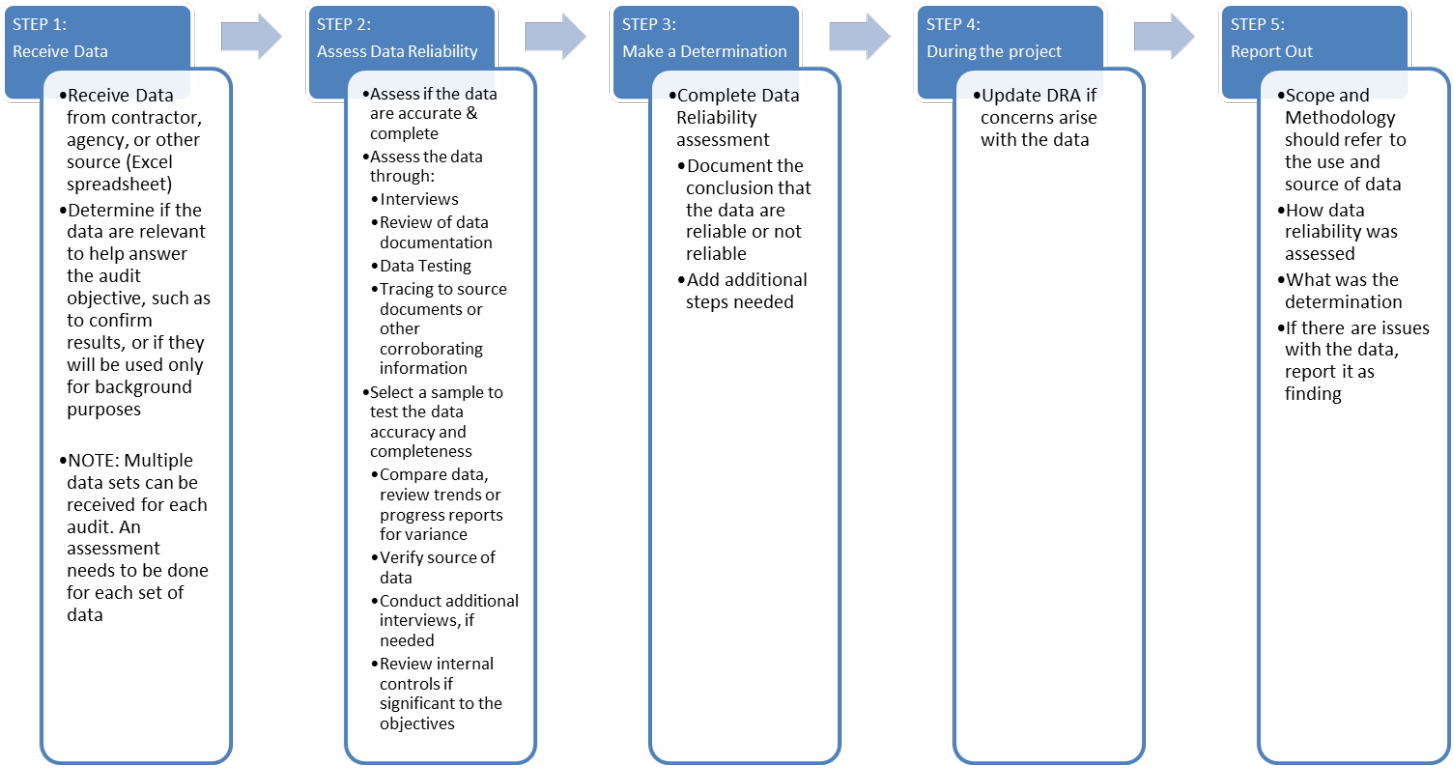
Is a DRA required to verify the $10 million figure? The number is background information and is separate from the objectives of the audit, as well as the fieldwork and findings. In this case, the DRA is not required.

[17] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 2: Deciding Whether a Data Reliability Assessment is Necessary, states that there may be cases where this is not true; these decisions should be made using professional judgment and documented in the project files, p.13.

The QA reviewer would not expect to see a DRA for background data.[18] However, the source of the data should be appropriately documented.

[18] GAO, *Assessing Data Reliability* (GAO-20-283G), Section 2: Deciding Whether a Data Reliability Assessment is Necessary, p.13.

APPENDIX B: ASSESSING DATA RELIABILITY FOR PERFORMANCE AUDITS



Source: QAWG

Note: This flowchart is not applicable to IT systems audits.

APPENDIX C: GLOSSARY

Audit: Either a financial audit or performance audit conducted in accordance with generally accepted government auditing standards (GAGAS) (GAS, 1.27b).

Audit Organization: A government audit entity or a public accounting firm or other audit entity that conducts GAGAS engagements. (GAS, 1.27c) Audit organization and Office of Inspector General (OIG)—that either with or without an audit function performs GAGAS engagements—are used interchangeably in this white paper.

Audit Risk: The possibility that the auditors' findings, conclusions, recommendations, or assurance may be improper or incomplete. The assessment of audit risk involves both qualitative and quantitative considerations. (GAS, 8.16)

Council of Inspector General on Integrity and Efficiency (CIGIE): An independent entity statutorily established within the executive branch by The Inspector General Reform Act of 2008, P.L. 110-409, to address integrity, economy and effectiveness issues that transcend individual Government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General. https://ignet.gov

Data: GAO refers to computer data as data (See GAO-20-283G). Therefore, when the term "data" is used, it includes computer-generated data. GAO's emphasis on data as evidence is the key takeaway for understanding the data reliability assessment. Reliability, a component of evidence quality (appropriateness), refers to verification and support (GAS, 8.102). Therefore, data are reliable to the extent they are verified and supported. This is the goal of a data reliability assessment.

Data Reliability Assessment (DRA): The process of assessing the reliability of the data for completeness and accuracy that is applicable to the audit process, in compliance with government auditing standards.

Federal Audit Executive Council (FAEC): A subgroup, established by CIGIE, to discuss and coordinate issues affecting the Federal audit community with special emphasis on audit policy and operations of common interest to FAEC members. https://ignet.gov/content/federal-audit-executive-council

GAO: *Government Accountability Office.* Known as "the investigative arm of Congress" and "the congressional watchdog," GAO supports Congress in meeting its constitutional responsibilities and helps improve the performance and accountability of the Federal government for the benefit of the American people.

GAO's Guidance: GAO's *Assessing Data Reliability* (GAO-20-283G). A guide (referred to as the **GAO's Guidance** in this white paper) published in December 2019 from GAO's Applied Research and Methods team that establishes a framework for data reliability assessment and

provides step-by-step guidance on the application of its principles.
https://www.gao.gov/assets/710/703275.pdf

Peer Review: OIG audit organizations are required by generally accepted government auditing standards (GAGAS) and CIGIE to have and conduct peer reviews to help auditors to fulfill their oversight roles and comply with statutory requirements, professional standards, and established policies and procedures.

Performance audits: Engagements that provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight to, among other things, improve program performance and operations, reduce costs, facilitate decision making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability. In a performance audit, the auditors measure or evaluate the subject matter of the audit and present the resulting information as part of, or accompanying, the audit report. (GAS, 1.21 and 8.14)

Professional Judgment: Use of the auditor's professional knowledge, skills, and abilities, in good faith and with integrity, to diligently gather information and objectively evaluate the sufficiency and appropriateness of evidence. Professional judgment includes exercising reasonable care and professional skepticism. (GAS, 3.110)

Quality Assurance (QA): An ongoing consideration and evaluation of the audit organization's system of quality control, including inspection of engagement documentation and reports for a selection of completed engagements to provide management with reasonable assurance that (1) the policies and procedures related to the system of quality control are suitably designed and operating effectively in practice and (2) auditors have followed professional standards and applicable legal and regulatory requirements. GAGAS also refers to this process as "monitoring of quality." (GAS, 5.47)

Quality Assurance (QA) Review: The performance, documentation, and communication of monitoring procedures and results that enable the audit organization to assess compliance with professional standards and quality control policies and procedures for completed GAGAS engagements. Reviews of the work by engagement team members prior to the date of the report are not monitoring procedures. (GAS, 5.43, 5.44, 5.47, 5.53, 5.59)

Quality Assurance (QA) Reviewer: An individual who performs monitoring procedures and assesses the audit organization's compliance with professional standards and quality control policies and procedures for GAGAS engagements. The individual should have sufficient expertise and authority with the audit organization and, if possible, does not have responsibility for the specific activity being reviewed. (GAS, 5.43, 5.48)

Quality Assurance Working Group (QAWG): A group formed by representatives from various Federal Offices of Inspector General in October 2016 to enhance and improve the quality assurance review processes within the Federal Inspector General community and that formally became a subgroup under the CIGIE FAEC in January 2019.
https://ignet.gov/sites/default/files/files/QAWG-Charter.pdf

Quality Control: The OIG's leadership and policies and procedures designed to provide the

audit organization with reasonable assurance that the organization and its personnel comply with professional standards and applicable legal and regulatory requirements. The nature, extent, and formality of an audit organization's quality control system will vary based on the audit organization's circumstances, such as size, number of offices and geographic dispersion, knowledge and experience of its personnel, nature and complexity of its engagement work, and cost-benefit considerations. (GAS, 5.02, 5.03)

U.S. Government Accountability Office's (GAO) *Government Auditing Standards*, 2018 Revision (April 2021), GAO-21-368G: This publication (known as the **Yellow Book** or **GAS**) prescribes professional standards that provide a framework for auditors to perform high-quality audit work with competence, integrity, objectivity, and independence to help improve government operations and services. These professional standards are often referred to as generally accepted government auditing standards (**GAGAS**).[19]
https://www.gao.gov/assets/gao-21-368g.pdf

[19] In April 2021, GAO made technical updates to the 2018 revision of Government Auditing Standards. These technical updates to the 2018 revision of Government Auditing Standards were effective upon issuance. For additional information, please see GAO-21-368G, pp. i-ii.

APPENDIX D: LIST OF CONTRIBUTORS

Team Member	Office of Inspector General
Richard McCaffery (Co-lead)	Pension Benefit Guaranty Corporation
Juana Morales (Co-lead)	U.S. Agency for International Development
Cheryl Chambers	Amtrak
Gary DeThomasis	Department of Veterans Affairs
Michelle Emigh	Department of Veterans Affairs
Ed Gold (Editor)	Amtrak
Glen Levis	Special Inspector General for Afghanistan Reconstruction
Whitney Miller	Amtrak
Nomi Taslitt	Special Inspector General for Afghanistan Reconstruction